

## WEILOVO PÁROVÁNÍ NA ELIPTICKÝCH KŘIVKÁCH V KRYPTOSYSTÉMECH ZALOŽENÝCH NA TOTOŽNOSTI A KRYPTOGRAFICKY RANDOMIZOVANÉ ODPOVÍDACÍ TECHNIKY

MIROSLAV KUREŠ

**ABSTRAKT.** Článek shrnuje dvě autorovy přednášky: o kryptografii založené na totožnosti a o kryptograficky randomizovaných odpovídacích technikách. V obou případech se opíráme o eliptickou kryptografii, tedy systémy využívající eliptické křivky nad konečnými poli. Hlavní účelem článku je poskytnout přehledný text demonstrující, s jakými algebraickými problémy se lze v eliptické kryptografii setkat a také, v případě randomizovaných odpovídacích technik, i poněkud nečekané užití kryptografického protokolu v dotazníkových šetřeních.

### ÚVOD

Text tohoto článku je členěn do dvou kapitol odpovídajících dvěma souvisejícím přednáškám autora: první se věnovala kryptografii založené na totožnosti, druhá kryptograficky randomizovaným odpovídacím technikám. Důraz je kladen na eliptickou kryptografii (ECC), již lze chápat i jako pojící bázi mezi tématy. Upření zájmu k ECC má své odůvodnění. Lze se totiž oprávněně domnívat, že nejpopulárnější algoritmus asymetrické kryptografie RSA je v současnosti také předmětem největšího úsilí o prolomení. ECC se opírá o řádově náročnější matematiku a přitom vykazuje i některé lepší vlastnosti (stejná bezpečnost s kratšími klíči).

Článek vyžaduje základní znalost kryptografických a některých algebraických pojmů a jistý vhled do problematiky.

#### 1. KRYPTOSYSTÉMY ZALOŽENÉ NA TOTOŽNOSTI A WEILOVO PÁROVÁNÍ NA ELIPTICKÝCH KŘIVKÁCH

##### 1.1. Kryptosystémy s veřejným klíčem ve srovnání s kryptosystémy založenými na totožnosti

Připomeňme nejprve základní parametry kryptosystémů s veřejným klíčem ve srovnání s kryptosystémy založenými na totožnosti za účasti v kryptografii již oblíbených osob: Alice, Boba a Evy.

---

2010 MSC. Primární 94A60, 68W20; Sekundární 14H52.

*Klíčová slova.* Kryptografie založená na eliptických křivkách, Weilovo párování, randomizované odpovídací techniky.

Práce byla podporována projektem A-Math-Net – Síť pro transfer znalostí v aplikované matematice (CZ.1.07/2.4.00/17.0100).

*Kryptosystém s veřejným klíčem:* je tvořen veřejným klíčem  $K_U$  a soukromým klíčem  $K_R$ . Klíč  $K_U$  je generován jednosměrnou funkcí z  $K_R$ . Pokud je Bob offline, nelze komunikovat. Pokud Eva ((wo)man-in-the-middle) přesvědčí Alici, že  $K_U$  je jiný, snadno pak dešifruje zprávy určené Bobovi. Tento *autentizační problém* (ověření identity) je řešen *certifikáty* poskytovanými *důvěryhodnou autoritou*.

*Kryptosystém založený na identitě:* veřejným klíčem  $K_U$  je jednoznačná identifikace Boba (např. telefonní číslo nebo e-mailová adresa). Certifikáty nejsou třeba. Je-li Bob offline, lze komunikovat (např. zpráva může čekat v *Short Message Service Center* a být odeslána později).

## 1.2. Eliptické křivky: základní pojmy

Dále uveďme základní pojmy kryptografie založené na eliptických křivkách.

**Eliptické křivky.** *Eliptickou křivkou*  $\mathcal{E}$  nad polem  $\mathbb{F}$  rozumíme algebraickou křivku třetího stupně s rovnicí

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

kde  $a_1, a_2, a_3, a_4, a_6 \in \mathbb{F}$  a kde tzv. *diskriminant*  $\Delta$  eliptické křivky  $\mathcal{E}$  je nenulový. Přitom

$$\begin{aligned} \Delta &= -d_2^2d_8 - 8d_4^3 - 27d_6^2 + 9d_2d_4d_6 \\ d_2 &= a_1^2 + 4a_2 \\ d_4 &= 2a_4 + a_1a_3 \\ d_6 &= a_3^2 + 4a_6 \\ d_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 + a_4^2. \end{aligned}$$

Je-li  $\mathbb{F}_q = \mathbb{F}_{p^n}$  ( $p$  prvočíslo,  $n \in \mathbb{N}$  konečné pole s charakteristikou různou od 2 a 3), pak vhodnou změnou souřadnic lze Weierstrassovu rovnici transformovat na rovnici

$$y^2 = x^3 + ax + b.$$

Je-li  $\mathbb{F}_q$  konečné pole s charakteristikou 2, pak vhodnou změnou souřadnic lze Weierstrassovu rovnici transformovat na rovnici

$$y^2 + xy = x^3 + ax^2 + b$$

(tzv. *nesupersingulární* eliptická křivka) nebo na rovnici

$$y^2 + cy = x^3 + ax + b$$

(tzv. *supersingulární* eliptická křivka). Obdobná věta platí i pro pole charakteristiky 3.

*Bodem eliptické křivky*  $\mathcal{E}$  rozumíme každý bod  $[x, y]$  se souřadnicemi  $x, y \in \mathbb{F}$  splňujícími její rovnici a dále bod  $\infty$ . Nad body eliptické křivky (nadále již bereme  $\infty \in \mathcal{E}$ ) lze zavést binární operaci značenou  $+$  a nazvanou *sečno-tečnové sčítání* takto: jsou-li dva body  $P = [x_1, y_1]$ ,  $Q = [x_2, y_2]$  eliptické křivky  $\mathcal{E}$  různé, vedeme skrze ně přímku; ta protne  $\mathcal{E}$  ještě v dalším bodě a  $R = P + Q$  vezmeme jako bod osově souměrný s tímto třetím bodem podle osy  $x$ . (Je-li přímka rovnoběžná s osou  $y$ , třetí bod  $\mathcal{E}$  na ní již neexistuje, pak klademe  $P + Q = \infty$ .) Dále, pro součet  $P + P$  vedeme bodem  $P$  tečnu; ta protne  $\mathcal{E}$  ještě v dalším bodě a  $R = P + P$  vezmeme jako bod osově souměrný s tímto bodem podle osy  $x$ . (Opět, je-li přímka

rovnoběžná s osou  $y$ , klademe  $P + P = \infty$ .) Součet libovolného bodu  $P$  eliptické křivky  $\mathcal{E}$  s bodem  $\infty$  položíme roven  $P$ .

Vzorce pro sečno-tečnové sčítání (pro pole s  $p$  různým od 2 i od 3):  
(případ  $R = P + Q$ ;  $R = [r_1, r_2]$ ,  $P = [p_1, p_2]$ ,  $Q = [q_1, q_2]$ )

$$r_1 = \left( \frac{q_2 - p_2}{q_1 - p_1} \right)^2 - p_1 - q_1 \quad r_2 = \left( \frac{q_2 - p_2}{q_1 - p_1} \right) (p_1 - r_1) - p_2$$

(případ  $R = 2P = P + P$ ;  $R = [r_1, r_2]$ ,  $P = [p_1, p_2]$ )

$$r_1 = \left( \frac{3p_1^2 + a}{2p_2} \right)^2 - 2p_1 \quad r_2 = \left( \frac{3p_1^2 + a}{2p_2} \right) (p_1 - r_1) - p_2$$

### 1.3. Eliptické křivky: vlastnosti grupy $(\mathcal{E}, +)$

Nyní je  $(\mathcal{E}, +)$  grupa. Řádem eliptické křivky  $\mathcal{E}$  pak rozumíme řád této grupy čili počet bodů  $\mathcal{E}$ ; značíme ho  $\#\mathcal{E}$ . Je-li  $\mathcal{E}$  eliptická křivka nad konečným polem  $\mathbb{F}_q$ , pro její řád  $\#\mathcal{E}(\mathbb{F}_q)$  platí odhad

$$q + 1 - 2\sqrt{q} \leq \#\mathcal{E}(\mathbb{F}_q) \leq q + 1 + 2\sqrt{q}$$

(Hasseho interval). Existuje tedy  $t \in \mathbb{Z}$  takové, že

$$\#\mathcal{E}(\mathbb{F}_q) = q + 1 - t, \quad \text{kde } |t| \leq 2\sqrt{q}.$$

Řád eliptické křivky lze pomocí  $t$  a Legendrova symbolu určit takto:

$$t = - \sum_{x \in \mathbb{F}_p} \left( \frac{x^3 + ax + b}{p} \right)$$

Přímé užití tohoto vztahu se nazývá *naivní algoritmus* pro určení řádu eliptické křivky.

**1.3.1. Torzní podgrupy.** Pro  $m \in \mathbb{N}$  bod  $P$  křivky  $\mathcal{E}$  splňující  $mP = \infty$  nazveme  *$m$ -tý torzní bod*. Množina všech  $m$ -tých torzních bodů se značí  $\mathcal{E}[m]$ , se zavedeným sčítáním bodů je  $\mathcal{E}[m]$  podgrupou grupy  $\mathcal{E}$ , nazýváme ji  *$m$ -tá torzní grupa*.

Je-li  $m$  libovolným násobkem řádu bodu  $P$ , pak  $P \in \mathcal{E}[m]$ . První torzní podgrupa je evidentně triviální (obsahuje pouze bod  $\infty$ ), zatímco  $\#\mathcal{E}$ -tá torzní podgrupa už je rovna  $\mathcal{E}$ . (Nic nového nepřináší, uvažujeme-li  $m > \#\mathcal{E}$ .) Bod  $\infty$  je prvkem všech  $m$ -tých torzních grup a dále je zřejmé, že v případě nesoudělného  $m$  a  $\#\mathcal{E}$  je také  $m$ -tá torzní podgrupa vždy triviální.

Jak vypadá druhá torzní grupa eliptických křivek? Pro její body platí  $P + P = \infty$ , což je možné jen pro nulovou  $y$ -ovou souřadnici bodu  $P$ . Tedy jde o to, zda existuje kořen rovnice  $x^3 + ax + b = 0$  (v  $\mathbb{F}_p$ ). Pokud ano, je řád  $\#\mathcal{E}(\mathbb{F}_p)$  sudý, a tedy  $t$  je sudé, neexistuje-li kořen  $x^3 + ax + b = 0$  (v  $\mathbb{F}_p$ ), je  $t$  liché.

Obecně nejsou torzní podgrupy grupy  $G$  cyklické, neboť sama grupa  $G$  nemusí být cyklická; nejsou cyklické ani pro případ  $m$ , které je menší než řád grupy  $G$ : například druhá torzní grupa grupy  $G = \mathbb{Z}_4 \oplus \mathbb{Z}_6$  je tvořena body  $(0, 0)$ ,  $(2, 0)$ ,  $(0, 3)$ ,  $(2, 3)$  a evidentně není generovaná jediným prvkem.

Pokud jde o grupu  $\mathcal{E}$  nad polem  $\mathbb{F}_q$ , pak ta je vždy izomorfní grupě  $\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$ , přičemž  $n_2$  dělí jak  $n_1$ , tak  $q - 1$  (Teorém 3.12, [6]). Pak ovšem  $\#\mathcal{E} = n_1 n_2$ . Je-li  $n_2 = 1$ , je grupa  $\mathcal{E}$  cyklická. Je-li  $n_2 > 1$  malé přirozené číslo  $(2, 3, 4, \dots)$ , říkáme,

že grupa  $\mathcal{E}$  je *téměř cyklická*. V cyklické grupě existuje bod, jehož řád je roven již přímo  $\#\mathcal{E}$ . Pro určení řádu eliptické křivky je ale také výhodné, je-li téměř cyklická, neboť v ní existují body dostatečně vysokého řádu, jejichž násobek patří do Hasseho intervalu.

#### 1.4. Eliptická kryptografie s veřejným klíčem

Uvedeme nyní, v čem spočívá podstata eliptické kryptografie s veřejným klíčem (ECC). Pro jednoduchost vezmeme prvočíselné pole  $\mathbb{F}_p$ , nad kterým uvažujeme eliptickou křivku  $\mathcal{E}$  a její bod  $P \in \mathcal{E}$ . Řádem bodu  $P$  rozumíme nejmenší  $n \in \mathbb{N}$  takové, že  $nP = \infty$ . Řád každého bodu  $P$  eliptické křivky  $\mathcal{E}$  dělí řád této křivky. (To je známý Lagrangeův teorém z teorie grup.) Bod  $P$  vyberme tak, aby jeho řádem bylo prvočíslo  $n$ . Dále vyberme nějaké  $k \in [1, n-1]$  a spočítáme  $Q = kP$ . Údaje o poli a eliptické křivce jsou tzv. *definiční parametry* a pokládají se za známé. Veřejným klíčem jsou body  $P$  a  $Q$  a soukromým klíčem číslo  $k$ .

ALGORITMUS. ZÁKLADNÍ ELGAMAL ŠIFROVÁNÍ POMOCÍ ELIPTICKÝCH KŘÍVEK.

VSTUP: DEFINIČNÍ PARAMETRY, VEŘEJNÝ KLÍČ  $P, Q$ , ZPRÁVA  $m$ .

VÝSTUP: ŠIFROVANÁ ZPRÁVA  $(C_1, C_2)$ .

1. Vyjádři  $m$  jako bod  $M$  eliptické křivky.
2. Vyber  $a \in [1, n-1]$ .
3. Spočti  $C_1 = aP$ .
4. Spočti  $C_2 = M + aQ$ .
5. Vrať  $(C_1, C_2)$ .

ALGORITMUS. ZÁKLADNÍ ELGAMAL DEŠIFROVÁNÍ POMOCÍ ELIPTICKÝCH KŘÍVEK.

VSTUP: DEFINIČNÍ PARAMETRY, VEŘEJNÝ KLÍČ  $P, Q$ , SOUKROMÝ KLÍČ  $k$ , ŠIFROVANÁ ZPRÁVA  $(C_1, C_2)$ .

VÝSTUP: ZPRÁVA  $m$ .

1. Spočti  $M = C_2 - kC_1$ .
2. Převeď  $M$  na  $m$ .
3. Vrať  $m$ .

#### 1.5. Bilineární zobrazení grup a Weilovo párování

Uvažujme dvě grupy  $G = (G, +)$ ,  $H = (H, \cdot)$ ,  $k \in \mathbb{Z}$ , a zobrazení  $\phi: G \times G \rightarrow H$  splňující

$$\begin{aligned}\phi(g_1 + g_2, g_3) &= \phi(g_1, g_3) \cdot \phi(g_2, g_3) \\ \phi(kg_1, g_2) &= (\phi(g_1, g_2))^k \\ \phi(g_1, g_2 + g_3) &= \phi(g_1, g_2) \cdot \phi(g_1, g_3) \\ \phi(g_1, kg_2) &= (\phi(g_1, g_2))^k.\end{aligned}$$

Takové zobrazení nazveme *bilineární zobrazení*. (Užíváme zde aditivní notaci pro  $G$  a multiplikativní notaci pro  $H$ .)

V případě eliptických křivek můžeme uvažovat např.  $G = (\mathcal{E}, +)$  a  $H = (\mathbb{F}_q - \{0\}, \cdot)$ , pro dále uvedené Weilova párování je volba grup speciálnější.

Weilovo párování je zobrazení

$$e: \mathcal{E}[m] \times \mathcal{E}[m] \rightarrow U_m,$$

kde  $U_m = (U_m, \cdot)$  je grupa  $m$ -tých odmocnin jedničky v  $\bar{\mathbb{F}}_p$  ( $\bar{\mathbb{F}}_p$  je algebraický uzávěr  $\mathbb{F}_q = \mathbb{F}_{p^n}$ ).

## 1.6. Weilovo párování v kryptografii založené na totožnosti

Důvěryhodná autorita je označována jako PKG (*private key generator*). Ta zvolí univerzální tajný klíč  $s$ . Poté zveřejní: rovnici eliptické křivky, její základní bod  $P$ , veřejný klíč systému  $sP$  a hašovací funkci  $h$ . Každý uživatel má veřejný klíč  $K_U = Q_{ID}$  (bod eliptické křivky vycházející z identity) a soukromý klíč  $K_R = sQ_{ID}$ , který obdrží od PKG. Odesílatel zprávy  $M$  vybere náhodně číslo  $r$  a posílá

$$(U, V) = (rP, M + h(e(Q_{ID}, sP)^r)).$$

Adresát pak za použití svého soukromého klíče  $sQ_{ID}$  z  $(U, V)$  spočte

$$M = V + h(e(sQ_{ID}, U)).$$

**1.6.1. Závěrečné poznámky k Weilovu párování.** Kryptografie založená na identitě je vhodná zejména pro šifrování mobilními telefony. Mezi eliptické křivky doporučené standardy patří

$$y^2 + xy = x^3 + x^2 + b$$

nad binárními poli  $\mathbb{F}_{2^{163}}$ ,  $\mathbb{F}_{2^{233}}$ ,  $\mathbb{F}_{2^{409}}$  (síla šifrování roste).

Např. pro  $q = 2^{409}$  musí  $n_2$  dělit jak  $n_1$ , tak některé z čísel

$$4480666067023,$$

$$76025626689833,$$

$$388119657591324467371942577087124648789568693795169094445383858 \backslash \\ 6764072695131586617955811936945129,$$

tzn. pro drtivou většinu křivek (cvičení: nebo pro všechny?) nad tímto polem je grupa eliptické křivky cyklická.

Bezpečnost kryptosystému založeného na identitě pak plyne z obtížnosti tzv. *Diffieho-Hellmanova problému pro cyklické grupy*.

## 2. RANDOMIZOVANÉ ODPOVÍDACÍ TECHNIKY A KRYPTOGRFICKY RANDOMIZOVANÉ ODPOVÍDACÍ TECHNIKY

### 2.1. Motivace pro nepřímé otázky a randomizaci

Kryptografie má zajímavé použití i v dotazníkových šetřeních. Uplatní se při řešení problému dotazování na záležitosti, u nichž lze očekávat, že respondent bude mít z nejrůznějších důvodů obavu odpovědět podle pravdy. Základní uvažovaná otázka je tato: *Patříte do („stigmatizované“) skupiny A?*

Z literatury věnující se problematice uveďme např. knihu [2], která je přehlednou monografií o randomizovaných technikách a technikách nepřímého dotazování.

## 2.2. Warnerova RRT

Klasická RRT (Warner 1965) vychází z následujícího schématu:

- $p_{\text{ct}}$  (známá) pravděpodobnost, že respondent odpoví na otázku pravdivě ( $> \frac{1}{2}$ , resp. stačí  $\neq \frac{1}{2}$ )
- $\pi_A$  skutečný podíl populace patřící do  $A$
- $p_{\text{yes}}$  podíl populace s odpovědí ano pak

$$p_{\text{yes}} = p_{\text{ct}}\pi_A + (1 - p_{\text{ct}})(1 - \pi_A);$$

pro  $N$  respondentů a  $L$  odpovědí ano je bodový odhad  $\widehat{p_{\text{yes}}}$  hodnoty  $p_{\text{yes}}$  roven  $\widehat{p_{\text{yes}}} = \frac{L}{N}$ , tzn. můžeme spočítat bodový odhad  $\widehat{\pi_A}$  hodnoty  $\pi_A$  jako

$$\widehat{\pi_A} = \frac{\widehat{p_{\text{yes}}} - (1 - p_{\text{ct}})}{2p_{\text{ct}} - 1} = \frac{p_{\text{ct}} - 1}{2p_{\text{ct}} - 1} + \frac{L}{N} \frac{1}{2p_{\text{ct}} - 1}.$$

$$\mathbb{E} \widehat{\pi_A} = \dots = \pi_A$$

$$\text{Var} \widehat{\pi_A} = \dots = \frac{1}{N} \left( \frac{1}{16(p_{\text{ct}} - \frac{1}{2})^2} - \left( \pi_A - \frac{1}{2} \right)^2 \right)$$

Předpokládejme, že například víme, že  $\frac{5}{6}$  populace odpovídá na každou otázku pravdivě a  $\frac{1}{6}$  vždy lže.

Potom  $p_{\text{yes}} \in [\frac{1}{6}, \frac{5}{6}]$ . Bude-li pak  $\widehat{p_{\text{yes}}} = \frac{2}{3}$ , je

$$\widehat{\pi_A} = \frac{\frac{2}{3} - (1 - \frac{5}{6})}{2 \cdot \frac{5}{6} - 1} = \frac{3}{4}$$

Protože obvykle nevíme, jaký podíl populace na otázku odpoví pravdivě a jaký podíl zalže, náhodně respondentovi vygenerujeme nebo si vygeneruje sám (*randomizace*), zda odpoví na otázku nebo na její negaci. Skutečnost, zda respondent odpovídá na otázku nebo na její negaci zůstane pro tazatele utajená, respondent o tomto utajení ví, a nemá proto důvod lhát.

Příklad:

*Otázka příslušnosti k A (otázka 1):* Přiznáváte, že jste se někdy dopustil daňového podvodu?

*Negace (otázka 2):* Můžete říct, že jste se nikdy nedopustil daňového podvodu?

Hodte si kostkou. Hodíte-li šestku, odpovězte na otázku 2. Hodíte-li něco jiného, odpovězte na otázku 1.

Dostaneme-li  $\frac{2}{3}$  odpovědí ano, máme

$$\widehat{\pi_A} = \frac{\frac{2}{3} - (1 - \frac{5}{6})}{2 \cdot \frac{5}{6} - 1} = \frac{3}{4}$$

## 2.3. Kryptograficky randomizovaná (Warnerova) odpovídací technika

Randomizace odpovědi respondenta nemusí být ponechána na respondentovi: může ji provést důvěryhodná autorita.

*CRRT protokol ideálního světa:*

$\mathcal{I}$  tazatel

$\mathcal{R}$  respondent

$\mathcal{T}$  důvěryhodná autorita

$$\mathcal{R} \xrightarrow{t_{\mathcal{R}}} \boxed{\Phi_{p_{\text{ct}}}(t_{\mathcal{R}}) = r_{\mathcal{R}}} \xrightarrow{r_{\mathcal{R}}} \mathcal{I}$$

(kde  $\Phi_{p_{\text{ct}}}(x)$  je randomizující funkce, jejímž výstupem je  $x$  s pravděpodobností  $p_{\text{ct}}$ )

V reálném světě je důvěryhodná autorita nahrazena kryptografickým protokolem. Pro ten se definují tři vlastnosti — požadavky:

- PR *soukromí respondenta*
- PI *soukromí tazatele*
- C *korektnost*
- slabý CRRT protokol: PR, C
- silný CRRT protokol: PR, PI, C

Nechť  $p$  je velké prvočíslo a  $q, q|(p-1)$ , jiné prvočíslo. Pak má  $\mathbb{Z}_p$  jedinou multiplikativní podgrupu  $G$  řádu  $q$ . Nechť  $g$  a  $h$  jsou dva z generátorů  $G$  (jejich vzájemné diskrétní logaritmy nejsou známy). Soukromý parametr:  $k = q$ , veřejný klíč  $K = (g, h)$ .

Zpráva  $\mu \in \mathbb{Z}_q$  je podepsána náhodným  $\rho \in \mathbb{Z}_q$  pomocí funkce

$$C_K(\mu, \rho) = g^\mu h^\rho.$$

$$p_{\text{ct}} = \frac{l}{n}$$

$$d = \left\lceil \frac{1}{1 - p_{\text{ct}}} \right\rceil$$

Idea protokolu spočívá ve skutečnosti, že alespoň jedno z čísel  $\mu + \nu + il \pmod n$  musí ležet v intervalu  $[0, d-1]$  a alespoň jedno z těchto čísel musí ležet v intervalu  $[l, n-1]$ .

PŘÍPRAVNÝ KROK:

- $\mathcal{R}$  vybere náhodně  $\mu$  z intervalu  $[0, n-1]$
- $\mathcal{I}$  vybere náhodně  $\nu$  z intervalu  $[0, n-1]$  a  $\sigma$  z intervalu  $[0, d-1]$

INTERAKTIVNÍ KROK:

- $\mathcal{R}$  spočte  $C_K(t_{\mathcal{R}}, \mu)$  a odešle výsledek  $\mathcal{I}$
- $\mathcal{I}$  spočte  $y = C_K(\sigma, \rho)$  pro náhodně vybrané  $\rho$ ;  $\nu$  a  $y$  odešle  $\mathcal{R}$  spolu s informací že  $y$  je  $C_K$ -funkcí nějakého  $i \in [0, d-1]$
- $\mathcal{R}$  verifikuje informaci; spočte hodnoty  $\mu'_i$  tak, že  $\mu'_i = t_{\mathcal{R}} \iff (\mu + \nu + il \pmod n) < l$ ; podepíše  $\sigma$  a pošle podpis spolu s  $\{\mu'_i\}$  pro všechna  $i \in [0, d-1]$ :  $[(\mu + \nu + il \pmod n) < l]$
- Potom  $\mathcal{I}$  položí  $r_{\mathcal{R}} = \mu'_\sigma$ ; to doplní podpisem  $\mathcal{R}$ , který může být ověřen  $\mathcal{R}$  i třetími stranami

## 2.4. Modifikované a zobecněné metody

**2.4.1. Greenbergova et al. metoda.** V Greenbergově metodě je negace otázky nahrazena jinou otázkou, často nesouvisející s předmětem výzkumu, *neškodnou*. Na tuto otázku se předpokládá pravdivá odpověď, pravděpodobnost odpovědi ano je známá, v nejjednodušší variantě je pak 1 nebo 0.

Příklad:

Otázka příslušnosti k  $A$  (otázka 1): Přiznáváte, že jste se někdy dopustil daňového podvodu?

Neškodná otázka (otázka 2): Padl vám při hodu mincí orel?

Hodte mincí. Padne-li vám orel, odpovězte na otázku 2. Padne-li vám hlava, odpovězte na otázku 1.

Dostaneme-li  $\frac{2}{3}$  odpovědí ano, máme

$$\widehat{\pi}_A = \frac{1}{2} \cdot \frac{2}{3} + \frac{1}{2} \cdot 1 = \frac{5}{6}.$$

**2.4.2. Polychotomická RRT.** V klasické RRT se zkoumá příslušnost ke skupině  $A$ : buď ano nebo ne (*dichotomická RRT*).

V *polychotomické RRT* může být odpovědí více, přičemž míra „stigmatizace“ může být různá.

Příklad.

Daňového podvodu jste se dopustil:

- zcela vědomě a úmyslně, pro vlastní obohacení
- z nedbalosti, pro zjednodušení administrativy, kvůli špatné evidenci dokladů, apod.
- nedopustil jsem se daňového podvodu

**2.4.3. Metoda tří karet.** Vyvinuta pro United States Government Accountability Office (GAO) pro zjištění počtu ilegálně usazeného (španělsky hovořícího) obyvatelstva. Respondenti určí svůj status postupně na třech kartách 1, 2 a 3, které vhazují do boxů  $A$ ,  $B$  a  $C$ . Citlivý status není nikdy v samostatné skupině, dochází ale k přeskupování.

**2.4.4. Závěrečné poznámky k použití různých kryptosystémů v CRRT.**

Navržený protokol je připraven (po případných modifikacích) k implementaci v různých kryptosystémech s veřejným klíčem. Připomeňme například, že v mobilní telefonii jsou užity kryptosystémy založené na eliptických křivkách (kvůli výrazně menší hardwarové náročnosti, než má nejrozšířenější RSA). Nabízí se zkusit zobecnit Pedersenovo schéma (pro  $\mathbb{Z}_p$ ) pro  $\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$ .

#### REFERENCE

- [1] A. Ambainis, M. Jakobsson, H. Lipmaa: *Cryptographic randomized response techniques*, v: Public Key Cryptography – PKC 2004, Vol. 2947 of Lecture Notes in Computer Science, 2004, 425–438.
- [2] A. Chaudhuri: *Randomized Response and Indirect Questioning Techniques in Surveys*, Chapman & Hall (CRC), Taylor & Francis, 2011.
- [3] J. A. Droitcour, E. M. Larson, F. J. Scheuren: *The three card method: Estimating sensitive survey items with permanent anonymity of response*, v: Proceedings of the American Statistical Association, Social Statistics Section, 2001.
- [4] B. G. Greenberg, A. A. Abul-Ela, W. R. Simmons, D. G. Horvitz: *The unrelated question randomized response model: Theoretical framework*, J. Amer. Statist. Assoc. **64** (1969), 520–539.
- [5] J. S. Hwu, R. J. Chen, Y.-B. Lin: *An efficient identity-based cryptosystem for end-to-end mobile security*, IEEE Transactions **5** (2006), 2586–2593.
- [6] D. Hankerson, A. Menezes, S. Vanstone: *Guide to Elliptic Curve Cryptography*, Springer, 2004.



- [7] R. Sakai, M. Kasahara: *ID based cryptosystems with pairing on elliptic curve*, Cryptology ePrint Archive, Report 2003/054.
- [8] S. L. Warner: *Randomized response: A survey technique for eliminating evasive answer bias*, J. Amer. Statist. Assoc. **60** (1965), 63–69.

Miroslav Kureš, Ústav matematiky, Fakulta strojního inženýrství, Vysoké učení technické v Brně, Technická 2, 616 69 Brno, Česká republika,  
*e-mail*: kures@fme.vutbr.cz